NCIS Warns Service Members About Card-Cracking Scams

Online Payment

All three methods involve requesting the service member provide online bank account login information; service members may also be asked to answer security questions established through their online bank account.

Department of Navy (DON) service members are facing severe financial losses after falling victim to card-cracking scams initiated via social media with promises of getting out of debt, making extra money, or improving credit scores.

There are three primary methods used to establish contact with potential victims. The first involves a social media post or message sent by a purported debt consolidator or business owner to lure service members into responding; the second involves the service member receiving a friend request from a person who shares many friends in common; and in the third method, the service member is presented with a copy of another service member's social media account to give the appearance of legitimacy and increase cooperation. After establishing contact, the service member receives a message from the scammer offering money as a "thank you" for their service or offering to pay money for their "debt relief."

Victims have reported that after the money is deposited directly into their accounts, the scammer then asks the victim to send a portion of the money via wire or cash to a third party. Victims then discover that loans have been opened in their name with the same financial institution. Any attempts to further contact the scammer are unsuccessful, leaving the victim to pay off the loan.

This online Card-Cracking scam continues to grow in the number of reported cases, and DON service members have realized large financial losses; some individuals have lost more than 40,000 USD to this scam. NCIS urges service members to never provide bank account login information or personally identifiable details to anyone. Reputable financial institutions and organizations will not contact you and request personally identifiable information.

If you suspect you've been targeted with this scam:

- Immediately discontinue correspondence with the suspected scammer.
- Notify your bank or financial institution and attempt to have your accounts locked.
- Change all account passwords and seek additional security steps by your financial institution.
- Consider a credit lock through one or all three of the major credit bureaus (Equifax, Experian, and Transunion).
- Enable two factor authentication for online accounts and mobile applications.
- Notify your respective command, NCIS office, and/or respective law enforcement authorities.

Submit suspected scams to NCIS using the NCIS Tips app or via www.ncis.navy.mil

NCIS